Beschreibung

Verfahren sowie Kommunikationsendgerät zum gesicherten Aufbau einer Kommunikationsverbindung

Die Erfindung betrifft ein Verfahren zum gesicherten Aufbau einer Kommunikationsverbindung gemäß dem Oberbegriff des Anspruchs 1 sowie ein Kommunikationsendgerät zum gesicherten Aufbauen einer Kommunikationsverbindung gemäß dem Anspruch 8.

Es sind Verfahren bekannt, um Daten über Kommunikationsnetze sicher transportieren zu können. Sicher bedeutet hierbei, dass Kommunikationsteilnehmer des Kommunikationsnetzes mit hoher Wahrscheinlichkeit darauf vertrauen können, dass empfangene Daten

1) auf dem Übertragungsweg nicht von jemand unbefugtem gelesen wurden,
2) auf dem Übertragungsweg nicht verändert wurden und
3) von demjenigen empfangen wurden, der die Daten gesendet zu haben vorgibt.

Die Sicherstellung dieser drei Grundprinzipen der sicheren Datenübertragung werden

1) Verschlüsselung (*"Ciphering"*)
2) Integritätsprüfung (*"Integrity Check"*) und
3) Authentifizierung (*"Authentication"*) genannt.

Grundsätzlich lassen sich für die Verschlüsselung und Authentifizierung genutzte Verfahren wie folgt in zwei Gruppen unterteilen:

Verfahren, bei denen die Schlüssel für Ver- und Entschlüsselung identisch sind (sog. symmetrische oder *"Secret Key"* Verfahren).

Verfahren, bei denen unterschiedliche Schlüssel für Ver- und Entschlüsselung genutzt werden (sog. asymmetrische oder "*Public Key*" Verfahren, bei denen ein privater Schlüssel, der sogenannte "*Private Key*" und ein öffentlicher Schlüssel "*Public Key*", d.h. ein Schlüsselpaar, je zu sichernder Einheit generiert wird).

Bei symmetrischen Verfahren ist im Allgemeinen der Algorithmus zur Ver- bzw. Entschlüsselung bekannt und für die wirksame Verschlüsselung kommt es auf die Geheimhaltung des Schlüssels an. Bei asymmetrischen Verfahren ist ebenfalls im Allgemeinen der Algorithmus bekannt und für die wirksame Verschlüsselung kommt es auf die Geheimhaltung des Private Key an, während der Public Key allgemein bekannt sein darf.

Haben zwei Kommunikationsendgeräte, die eines der o.g. Verfahren nutzen wollen, und die denselben Algorithmus für dieses Verfahren betreiben, einen geeigneten Schlüssel ausgetauscht, und ist dieser Schlüssel niemandem (keiner unautho-
20 risierten Einheit) bekannt, so gewährleistet der Verschlüsselungsalgorithmus eine ausreichende Verschlüsselung bzw. Authentifizierung oder Integritätsprüfung.

Eine überaus sichere Kommunikation lässt sich in solchen Kommunikationsnetzen gewährleisten, in denen, wie beschrieben, Algorithmen für die Übertragungssicherheit sorgen und in denen den kommunizierenden Einheiten die Schlüssel bereits vor Beginn der Datenkommunikation bekannt sind.

Dagegen stellt in Netzen, in denen die Schlüssel zunächst vor der Datenübertragung ausgehandelt werden müssen, diese Schlüsselaushandlungsphase eine Möglichkeit für unauthorisierte Kommunikationseinheiten dar, die Schlüssel zu erhalten oder zu manipulieren und somit die sichere Datenübertragung zu korrumpieren.

Insbesondere bei solchen Datenübertragungen, bei denen die Kommunikationseinheiten (Kommunikationsendgeräte) zunächst kein Wissen voneinander haben, bei denen sie also auch keine Schlüssel oder gemeinsamen unveröffentlichten geheime Daten haben, müssen am Anfang der Datenübertragung Nachrichten ausgetauscht werden, die weitgehend unverschlüsselt sind und somit einem Angriff durch unauthorisierte Dritte ausgesetzt sein können. Solche Dritte könne dann ggf. die Schlüsselaushandlung abhören und sich so der Schlüssel bemächtigen, oder sie geben sich jeder der Kommunikationseinheiten als die jeweils andere aus ("*Man in the middle*") und können so die Kommunikation zwischen den beiden Einheiten abhören.

Die der Erfindung zugrundeliegende Aufgabe ist es, ein Verfahren bzw. ein Kommunikationsendgerät anzugeben, die es erlauben, unberechtigte Zugriffe auf innerhalb eines Kommunikationsnetzes übertragenen Daten weitestgehend auszuschließen.

Diese Aufgabe wird ausgehend von dem Verfahren gemäß dem Oberbegriff des Anspruchs 1 durch dessen kennzeichnenden Merkmale gelöst. Zudem wird die Aufgabe durch das Kommunikationsgerät gemäß dem Oberbegriff des Anspruchs 8 gelöst.

Bei dem erfindungsgemäßen Verfahren zum gesicherten Aufbau einer, insbesondere direkten, gemäß einem ersten Kommunikationsstandard funktionierenden ersten Kommunikationsverbindung zwischen zumindest einem ersten Kommunikationsendgerät und einem zweiten Kommunikationsendgerät, wobei zum Etablieren der direkten Kommunikationsverbindung gemäß dem ersten Kommunikationsstandard zwischen dem ersten Kommunikationsendgerät und dem zweiten Kommunikationsendgerät ein Austausch von Schlüsseln zur Verschlüsselung von über die direkte Kommunikationsverbindung übertragenen Daten durchgeführt wird, erfolgt der Schlüsselaustausch zumindest teilweise über eine zweite gemäß einem Funkkommunikationsstandard vermittelte, insbesondere dem UMTS-Standard, funktionierende Kommunikationsverbindung.

Das erfindungsgemäße Verfahren hat zudem den Vorteil, dass sie in allen Kommunikationssystemen, in denen Endgeräte direkt oder zumindest über ein unsicheres Kommunikationsnetz miteinander kommunizieren, beispielsweise Funkgeräte, DECT Geräte, WLAN oder LAN Kommunikation oder auch UMTS Mobilfunkgeräte im sogenannten "Direct Mode", einer Endgerät-zu-Endgerät Kommunikation ohne Mobilfunknetz, die eine mögliche Erweiterung des UMTS Standards für die Zukunft darstellt, Anwendung finden kann, da zumindest Teile der Schlüssel über einen gesicherten Übertragungsweg zu den Kommunikationspartnern gelangen.

Vorzugsweise erfolgt der Schlüsselaustausch nach Eingehen einer vom zweiten Kommunikationsendgerät gesendeten ersten Nachricht beim ersten Kommunikationsendgerät, wobei hierzu die erste, insbesondere als Anfrage "Request" ausgestaltete, Nachricht eine das zweite Kommunikationsendgerät in einem, nach dem Funkkommunikationsstandard ausgestalteten, Netz eindeutig authentifizierenden Adressinformation enthält, so dass zum einen klar ist, dass der Wunsch des Aufbaus einer direkten Kommunikation erfasst und durch das Übertragen der Adressinformation sichergestellt wird, dass nur der hierdurch im gemäß dem Funkkommunikationsstandard ausgestaltete Kommunikationspartner authentifiziert und in der Lage ist, Daten über den zweiten Kommunikationsweg zu erhalten.

Wird durch das erste Kommunikationsendgerät eine zweite Nachricht, die einen ersten Schlüssel enthält, an das zweite Kommunikationsendgerät über die zweite Kommunikationsverbindung übermittelt und durch das zweite Kommunikationsendgerät anschließend eine dritte Nachricht, die einen zweiten Schlüssel enthält, an das erste Kommunikationsendgerät über die erste Kommunikationsverbindung übermittelt, ist zumindest die Übertragung des ersten Schlüssels gesichert und damit zumindest das Manipulieren bzw. Korrumpieren von Daten, die vom zweiten Kommunikationsendgerät zum ersten Kommunikationsendgerät

übermittelt werden, weitestgehend ausgeschlossen. Diese Variante berücksichtigt den Effekt, dass im Allgemeinen für einen Missbrauch der übertragenen Daten, beide Übertragungsrichtungen abgehört und vor allem entschlüsselt werden müssen. Ist zumindest eine Übertragungsrichtung vor dem Abfangen des Schlüssels und damit vor dem Abhören gesichert, fällt es einem unberechtigten schwer, den Kontext der ausgetauschten Daten nachzuvollziehen. Ein "Man in the middle" Angriff, ist so nicht möglich.

Bei einer vorteilhaften Weiterbildung übermittelt sowohl das erste Kommunikationsendgerät eine zweite Nachricht, die einen ersten Schlüssel enthält, an das zweite Kommunikationsendgerät als auch das zweite Kommunikationsendgerät eine dritte Nachricht, die einen zweiten Schlüssel enthält, an das erste Kommunikationsendgerät über die zweite Kommunikationsverbindung, so dass der Schlüssel für beide Übertragungsrichtungen vor einem Abfangen geschützt sind.

Wird mit der zweiten Nachricht neben dem ersten Schlüssel eine, insbesondere zufallsgenerierte, Bitfolge an das zweite Kommunikationsgerät über die zweite Kommunikationsverbindung übertragen, hat dies den Vorteil, dass das erste Kommunikationsendgerät durch eine nur ihr bekannte Bitfolge eine Authentifizierungsmöglichkeit schafft. Zum Schutz vor Entzifferung durch unberechtigte Dritte, wird die vom zweiten Endgerät empfange Bitfolge, vorteilhafter Weise mit dem ersten Schlüssel des zweiten Kommunikationsendgerätes verschlüsselt über die erste Kommunikationsverbindung als Teil der dritten Nachricht übertragen, so dass im ersten Kommunikationsendgerät ein Vergleich der Bitfolge der zweiten Nachricht mit der Bitfolge der dritten Nachricht erfolgen kann, dessen Ergebnis Aufschluss über die Authentisierung gibt. Denn bei einer Übereinstimmung der beiden Abfolgen ist klar, dass der Ursprung der dritten Nachricht nur das zweite Kommunikationsendgerät sein kann, so dass letztendlich der gewünschte Datenaustausch zwischen dem ersten Kommunikationsendgerät und

zweiten Kommunikationsendgerät auf direktem Weg, d.h. über die erste Kommunikationsverbindung erfolgen kann, wobei hierzu vom ersten Kommunikationsendgerät ausgehenden Daten mit dem zweiten Schlüssel und die vom zweiten Kommunikationsendgerät ausgehenden Daten mit dem ersten Schlüssel verschlüsselt werden, so dass unberechtigtes Auswerten der übertragenen Daten verhindert wird.

Funktioniert das Übermitteln der zweiten und/oder dritten Nachricht gemäß einem Standard für über Funk versendete Kurzmitteilungen, insbesondere nach dem "Short Message Standard", erfolgt die Umsetzung des Verfahrens auf einfache Art unter Ausnutzung vorhandener Ein-Wege Messaging Methoden.

Alternativ lässt sich das Übermitteln der zweiten und/oder dritten Nachricht gemäß einem Standard zum Übertragen von Paketdaten realisieren, so dass das erfindungsgemäße Verfahren beispielsweise in Systemen ohne vergleichbare Ein-Weg Messaging Methoden implementiert werden kann.

Das Kommunikationsendgerät zum gesicherten Aufbau einer, insbesondere direkten, Kommunikationsverbindung, gemäß Anspruch 8 ermöglicht eine Realisierung des Verfahrens durch Bereitstellung von Mitteln zur Durchführung des Verfahrens.

Weitere Einzelheiten und Vorteile der Erfindung, werden in den Figuren 1 bis 2 erläutert. Davon zeigen

Figur 1 Darstellung eines Anordnungsszenarios,

Figur 2 schematische Darstellung des Ablaufs des erfindungsgemäßen Verfahrens bei einem Einsatz in einer Anordnung gemäß dem Szenario.

Bei dem in Figur 1 dargestellten Beispiel ist ein erstes Kommunikationsendgerät PC1 und ein zweites Kommunikationsendgerät PC2, die bei diesem Ausführungsbeispiel als Datenverar-

beitungsendgerät, beispielsweise Personal Computer (PC) oder Laptop, mit jeweils einer UMTS-PC-Karte UMTS1, UMTS2 ausgestaltet sind.

Mit Hilfe dieser UMTS-PC-Karten UMTS1, UMTS2 sind das erste Kommunikationsendgerät PC1 und das zweite Kommunikationsendgerät PC2 in der Lage, einem durch ein UMTS-Mobilfunknetz UMTS-NETZWERK bereitgestellte Funkversorgungsbereich Daten drahtlos zu übertragen. Das UMTS-Moilfunknetz UMTS-NETZWERK ist für diese Darstellung vereinfacht durch UMTS-Luftschnittstellen (Pfeile) und einem *Radio Network Controler* (RNC), der die Luftschnittstellen kontrolliert, dargestellt.

Zwischen den beiden Kommunikationsendgeräten PC1, PC2 gemäß dem Ausführungsbeispiel besteht zusätzlich noch eine gemeinsame Anbindung an ein weiteres Kommunikationsnetzwerk LAN. Über dieses, als sogenanntes "Local Area Network" ausgestaltetes, Netzwerk LAN sind das erste Kommunikationsendgerät PC1 und das zweite Kommunikationsendgerät PC2 in der Lage, eine direkte Verbindung zueinander aufzubauen, direkt heißt hierbei, dass ohne Vermittlung einer übergeordneten, bei drahtlosen Netzen mit einer Basisstation vergleichbaren, Instanz eine Kommunikationsverbindung etabliert und hierüber Daten ausgetauscht werden können.

Die Erfindung ist alternativ auch mit mobilen Endgeräten wie UMTS Endgeräten, die zu einer direkten Verbindung in einem sogenannten "Direct Mode" befähigt sind, oder "Digital European Cordless Telefone" DECT Endgeräten in einem vergleichbaren "Direct Mode" realisierbar aber nicht darauf eingeschränkt. Denkbar wäre beispielsweise die Anwendung des Kurzstreckenfunkstandards Bluetooth zur Realisierung einer direkten Verbindung.

Für dieses Ausführungsbeispiel ist, ohne hierauf eingeschränkt zu sein, als Funkkommunikationsnetzwerk das UMTS-Netz gewählt, da es eine gesicherte Kommunikation zwischen

zwei Teilnehmern ermöglicht. Vergleichbar sichere Funkkommunikationsnetzwerke wären ebenso vorteilhaft einsetzbar.

Der erfindungsgemäße Ablauf eines Aufbaus einer gesicherten direkten Verbindung in oben dargestelltem Szenario ist in Figur 2 gezeigt.

Ein wesentliches Merkmal des erfindungsgemäßen Verfahrens ist es, dass die beiden Kommunikationsendgeräte zusätzlich zu der zu etablierenden direkten Kommunikationsmöglichkeit über das lokale Netz LAN , auch über die Möglichkeiten der Kommunikation über ein gesichertes Funkkommunikationsnetz, wie das UMTS-Mobilfunknetz UMTS-NETZWERK verfügen, wobei den Engeräten vorteilhafter Weise innerhalb des betreffenden Funkkommunikationsnetzwerks UMTS-NETZWERK jeweils eine eineindeutige Adresse zugeordnet sein muss.

Das Verfahren kommt dann zu tragen, wenn beispielsweise das zweite Kommunikationsendgerät PC2 feststellt, dass es eine gesicherte Kommunikationsstrecke mit dem ersten Kommunikationsendgerät PC1 aufbauen möchte.

Ein mögliches Szenario ist beispielsweise, dass es sich bei dem ersten Kommunikationsendgerät PC1 um einen Server im Internet handelt, der beispielsweise den Internet-Vertrieb einer Firma unterstützt.

Das zweite Kommunikationsendgerät PC2 sei dann beispielsweise der Personal Computer eines Nutzers, der Produkte dieser Firma über das Internet erwerben möchte. Dazu schaut der Nutzer auf der Homepage der Firma nach und sieht dort die Telefonnummer A1 (MS-ISDN) des Servers, die für elektronische Schlüsselaushandlungen genutzt werden soll (bspw. +491755815000).

Diese Telefonnummer kann er entweder per Hand oder automatisch in ein entsprechendes Programm seines Endgerätes PC1

eingeben, welches die erfindungsgemäße verschlüsselte Kommunikation leisten soll.

Das erfindungsgemäße Verfahren beginnt nun mit einem ersten Schritt 1, bei dem das zweite Kommunikationsendgerät PC2 eine Aufforderungsnachricht REQ zusammenstellt, die die Telefonnummer A2 vom zweiten Endgerät PC2 im UMTS-Netz (MS-ISDN, bspw. +491755815099) und die Anforderung eines Schlüssels enthält, und sendet diese über das Internet LAN an das erste Kommunikationsendgerät PC1.

In einem zweiten Schritt 2 empfängt das erste Kommunikationsendgerät PC1 diese Nachricht, generiert ein Schlüsselpaar, bestehend aus einem privaten 128 Bit langen ersten Schlüssel PRIVAT1 und einem öffentlichen 128 Bit langen zweiten Schlüssel PUBLIC1. Des Weiteren generiert das erste Endgerät eine 32 Bit lange zufällige Bitfolge TOKEN.

Die Zufallsfolge TOKEN und sowie der zweite Schlüssel PUBLIC1 werden in einem dritten Schritt 3 in eine erste Nachricht M1, die nach dem aus dem "Global Sytem Mobile" GSM und UMTS Standard bekannten "Short Message Service(SMS)" ausgestaltet ist, über das UMTS Mobilfunknetz UMTS-NETZ an das zweite Kommunikationsendgerät PC2 gesendet.

In einem vierten Schritt 4 empfängt das zweite Kommunikationsendgerät PC2 diese SMS und vergleicht die Absender-Rufnummer A1 mit der Rufnummer aus dem Internet (hier +491755815000). Stimmen diese überein, ist vorteilhafterweise der Absender der SMS authentifiziert, so dass in diesem vierten Schritt 4 das zweite Kommunikationsendgerät PC2 seinerseits ein Schlüsselpaar mit einem privaten 128 Bit langen dritten Schlüssel PRIVATE2 und einem öffentlichen 128 Bit langen vierten Schlüssel PUBLIC2 generiert und eine zweite Nachricht M1 zusammenstellt.

In einem fünften Schritt 5 wird die zweite Nachricht M1, in der der vierte Schlüssel PUBLIC2 gemeinsam mit der zuvor erhaltenen Zufallsfolge TOKEN, welche zuvor mit dem zweiten Schlüssel, das mit PUBLIC1 verschlüsselt wurde, enthalten ist, über die durch das Internet zur Verfügung gestellte direkte Verbindungsmöglichkeit an das erste Endgerät PC1 übertragen.

Nach Empfang dieser zweiten Nachricht M2 kann das erste Kommunikationsendgerät PC1 die darin enthaltene Zufallsfolge TOKEN mit Hilfe vom ersten Schlüssel PRIVATE 1 entschlüsselt werden, um durch einen Vergleich mit der zuvor übermittelten Zufallsfolge TOKEN den Absender der zweiten Nachricht M2 zu authentifizieren.

Stimmen diese Folgen überein, kann die angestrebte direkte Verbindung zwischen dem ersten Kommunikationsendgerät PC1 und dem zweiten Kommunikationsendgerät PC2 gesichert durchgeführt werden, da nach Abschluss des erfindungsgemäßen Verfahrens, neben der Authentisierung der Quelle PC1, PC2 auch die ausgehandelten Schlüssel PUBLIC1, PUBLIC2 für eine Verschlüsselung der direkten Kommunikation zwischen dem ersten Endgerät PC1 und dem zweiten Endgerät PC2 beim jeweiligen Kommunikationspartner zur Verfügung stehen.

Die Erfindung soll nicht auf das beschriebene Ausführungsbeispiel beschränkt sein. Vielmehr umfasst sie auch die Anwendung in allen Kommunikationssystemen, in denen Endgeräte direkt oder zumindest über ein unsicheres Kommunikationsnetz miteinander kommunizieren, wie beispielsweise Funkgeräte, DECT Geräte, zur WLAN-Kommunikation ausgestaltete Geräte oder auch UMTS Mobilfunkgeräte im sogenannten "Direct Mode", einer Endgerät-zu-Endgerät Kommunikation ohne Mobilfunknetz, die eine mögliche Erweiterung des UMTS Standards für die Zukunft darstellt, sofern der erfindungswesentliche Kern (zumindest teilweiser Schlüsselaustausch für eine Kommunikation über ei-

ne Kommunikationsverbindung, die gemäß einem gesicherten Funkkommunikationsstandard funktioniert, implementiert ist.

Patentansprüche

1. Verfahren zum gesicherten Aufbau einer, insbesondere direkten, gemäß einem ersten Kommunikationsstandard funktionierenden ersten Kommunikationsverbindung zwischen zumindest einem ersten Kommunikationsendgerät und einem zweiten Kommunikationsendgerät, wobei zum Etablieren der direkten Kommunikationsverbindung gemäß dem ersten Kommunikationsstandard zwischen dem ersten Kommunikationsendgerät und dem zweiten Kommunikationsendgerät ein Austausch von Schlüsseln zur Verschlüsselung von über die direkte Kommunikationsverbindung übertragenen Daten durchgeführt wird, dadurch gekennzeichnet, dass der Schlüsselaustausch zumindest teilweise über eine zweite gemäß einem Funkkommunikationsstandard vermittelte, insbesondere dem UMTS-Standard, funktionierende Kommunikationsverbindung erfolgt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schlüsselaustausch nach Eingehen einer vom zweiten Kommunikationsendgerät gesendeten ersten Nachricht beim ersten Kommunikationsendgerät erfolgt, wobei hierzu die erste, insbesondere als Anfrage "Request" ausgestaltete, Nachricht eine das zweite Kommunikationsendgerät in einem, nach dem Funkkommunikationsstandard ausgestalteten, Netz eindeutig authentifizierenden Adressinformation enthält.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass das erste Kommunikationsendgerät eine zweite Nachricht, die einen ersten Schlüssel enthält, an das zweite Kommunikationsendgerät über die zweite Kommunikationsverbindung übermittelt und das zweite Kommunikationsendgerät anschließend eine dritte Nachricht, die einen zweiten Schlüssel enthält, an das erste Kommunikationsendgerät über die erste Kommunikationsverbindung übermittelt.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass das erste Kommunikationsendgerät eine zweite Nachricht, die einen ersten Schlüssel enthält, an das zweite Kommunikationsendgerät über die zweite Kommunikationsverbindung übermittelt und das zweite Kommunikationsendgerät eine dritte Nachricht, die einen zweiten Schlüssel enthält, an das erste Kommunikationsendgerät über die zweite Kommunikationsverbindung übermittelt.

5. Verfahren nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass
   a) mit der zweiten Nachricht neben dem ersten Schlüssel eine, insbesondere zufallsgenerierte, Bitfolge an das zweite Kommunikationsgerät über die zweite Kommunikationsverbindung übertragen wird,
   b) die Bitfolge, mit dem ersten Schlüssel des zweiten Kommunikationsendgerätes verschlüsselt und über die erste Kommunikationsverbindung als Teil der dritten Nachricht übertragen wird,
   c) im ersten Kommunikationsendgerät ein Vergleich der Bitfolge der zweiten Nachricht mit der Bitfolge der empfangenen dritten Nachricht erfolgt,
   d) bei einer Übereinstimmung ein Datenaustausch zwischen dem ersten Kommunikationsendgerät und zweiten Kommunikationsendgerät über die erste Kommunikationsverbindung stattfindet, wobei hierzu vom ersten Kommunikationsendgerät ausgehenden Daten mit dem zweiten Schlüssel und die vom zweiten Kommunikationsendgerät ausgehenden Daten mit dem ersten Schlüssel verschlüsselt werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Übermitteln der zweiten und/oder dritten Nachricht gemäß einem Standard für über Funk versendete Kurzmitteilungen, insbesondere nach dem "Short Message Standard", funktioniert.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Übermitteln der zweiten und/oder dritten Nachricht gemäß einem Standard zum Übertragen von Paketdaten funktioniert.

8. Kommunikationsendgerät zum gesicherten Aufbau einer, insbesondere direkten, Kommunikationsverbindung, insbesondere nach einem der vorhergehenden Ansprüche, gekennzeichnet durch Mittel zur Durchführung des Verfahrens.

Zusammenfassung

Verfahren sowie Kommunikationsendgerät zum gesicherten Aufbau einer Kommunikationsverbindung

Bei dem erfindungsgemäßen Verfahren zum gesicherten Aufbau einer, insbesondere direkten, gemäß einem ersten Kommunikationsstandard funktionierenden ersten Kommunikationsverbindung zwischen zumindest einem ersten Kommunikationsendgerät und einem zweiten Kommunikationsendgerät, wobei zum Etablieren der direkten Kommunikationsverbindung gemäß dem ersten Kommunikationsstandard zwischen dem ersten Kommunikationsendgerät und dem zweiten Kommunikationsendgerät ein Austausch von Schlüsseln zur Verschlüsselung von über die direkte Kommunikationsverbindung übertragenen Daten durchgeführt wird, erfolgt der Schlüsselaustausch zumindest teilweise über eine zweite gemäß einem Funkkommunikationsstandard vermittelte, insbesondere dem UMTS-Standard, funktionierende Kommunikationsverbindung.

Figur 2